(19)

(11) Publication number: **05298174**

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: **04101355**

(51) Intl. Cl.: **G06F 12/00** G06F 12/00 G06F 13/00

(22) Application date: **21.04.92**

(30) Priority:

(43) Date of application publication: **12.11.93**

(84) Designated contracting states:

(71) Applicant: **TOSHIBA CORP**

(72) Inventor: **NUKUI HARUMI**

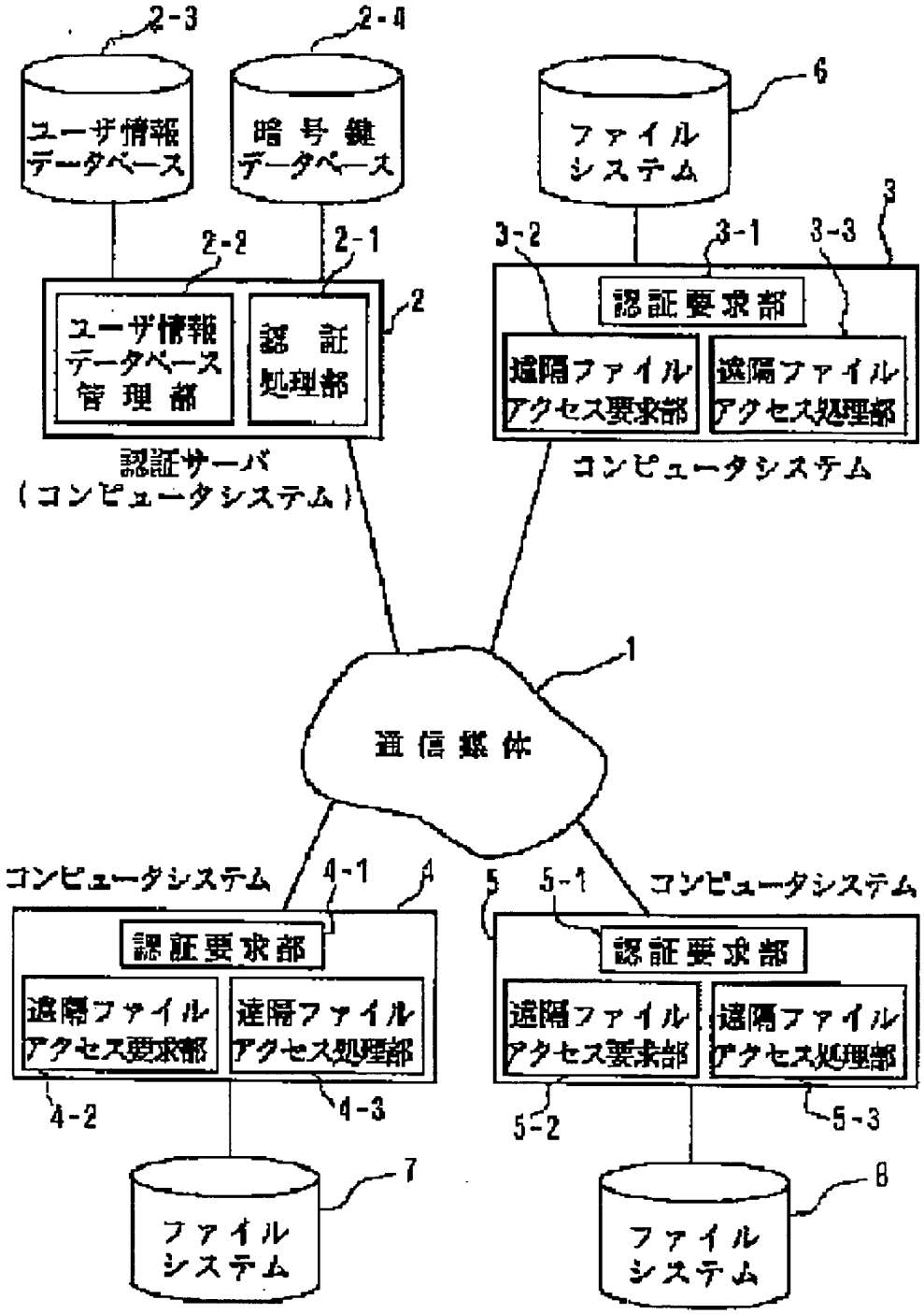
(74) Representative:

(54) REMOTE FILE ACCESS SYSTEM

(57) Abstract:

PURPOSE: To improve the justification and safety of a file access.

CONSTITUTION: A remote file access request part 3-2 of a computer system 3 to be a remote file access request origin ciphers the authenticated certificate and the access request list acquired by the authentication server (computer system) 2 by a self-decoding key, prepares an access request packet by adding user identification information to the ciphered information, further ciphers it by the ciphering key of an access request destination computer system, and performs the access request of a remote file. A remote file access processing part 4-3 of a computer system 4 to be a remote file access request destination decodes the ciphered access request packet by the self-decoding key, acquires the ciphering key of a user from the authentication server 2 based on the user identification information obtained by further decoding, decodes the authenticated certificate and the access request list and performs the authentication of the user and the processing for the acceptance and rejection of the remote file access.



(Translation of Citations)

Citation A

Japanese Patent Application Public-disclosure No. 5-298174
Japanese Patent Application Public-disclosure date: November 12, 1993
Japanese Patent Application No. 4-101355
Japanese Patent Application date: April 21, 1992
Title of the invention: Remote file access system
Gist of the invention:
[Industrial use of the invention]

The present invention is directed to a remote file access system for accessing a remote file system on a network system consisting of a plurality of computer systems connected to one another via a communication medium.

[Embodiment]

Hereafter, an embodiment of the present invention will be specifically described with reference to the attached drawings.

Fig. 1 is a schematic block diagram of a remote file access system in accordance with an embodiment of the present invention. In Fig. 1, a plurality of computer systems 2 ~ 5 are connected to communication medium 1. The computer system 2 is an authentication server and consists of user information database control means 2-2 for collectively managing user information on the network and authentication processing means 2-1 for issuing an authentication certificate for determining whether a user is authorized to utilize a service. Further, user information database 2-3, for managing user information and service information that a user can utilize on the network, and cryptographic key database 2-4, are connected to the computer system 2. The computer systems 3 ~ 5 are computer systems used by ordinary users, as opposed to a computer system which serves as an authentication server, and they consist of authentication request means 3-1 ~ 5-1 for inputting user information such as user names and passwords, remote file access request means 3-2 ~ 5-2 for making a request to the other computer systems for service and remote file access processing means 3-3 ~ 3-5 for receiving requests for service from other computer systems,

respectively. The remote file access processing means 3-3 ~ 5-3 have access authorization lists of the file systems 6 ~ 8.

Fig. 2 is a schematic flow chart describing the procedure for remote file access. In Fig. 2, the authentication request means 3-1 ~ 5-1 of the computer systems 3 ~ 5 request the authentication processing means 2-1 of the authentication server 2 to identify a user on the basis of a user name and a password entered by the user. Once the identity of the user is verified and an authentication certificate is issued to the user, it is determined that the user has completed the service utilization start procedures (step 21). Next, the authentication certificate is saved in the computer systems 3 ~ 5. On the basis of the authentication certificate, the remote file access request means 3-2 ~ 5-2 of the computer systems 3 ~ 5 make a request for remote file access (step 22). In response to the request, the remote file access processing means 3-3 ~ 3-5 of the computer systems 3 ~ 5 check to see if the requested file access is authorized (step 23). If yes, file access is conducted upon verification of the authentication certificate.

Fig. 3 illustrates a format of an authenticated certificate. In Fig. 3, a host name of an authentication server and an address representing the location of the authentication server are stored in the authentication certificate. In addition to a host name and an address, a user name, user ID number representing identity of a user, time of issuance of the authentication certificate and expiration date of the authentication certificate are also stored. On the basis of the authentication certificate, the remote file access request means of the computer systems make remote file access.

Next, a description is provided of how a user of the computer system 3, to whom an authentication certificate is issued, makes a request for access to a file of the computer system 4. The remote file access request means 3-2 of the computer system 3 assembles an access request packet and transfers the packet to the remote file access processing means 4-3 of the computer system 4, which is a target node, whereby the remote file access request is made.

Fig. 4 illustrates a configuration of an access request packet. In Fig. 4, the authentication certificate and access request list in the diagonally shaded area 41 are encrypted with a decryption key of a requesting user of the computer system 3, and as is indicated by the diagonally shaded area 40, the entire access request packet is encrypted with an encryption key of the

computer system 4, which is a remote node. The access request list contains a name of a target file and a type of access.

Fig. 5 is a flow chart describing the procedure for an operation of the remote file access request means. In Fig. 5, upon receiving an authentication certificate from the authentication server 2, the remote file access request means 3-2 of the computer system 3 prepares an access request list for the remote file of the computer system 4 as a remote node (step 51). Next, an encryption key of a remote node to be file-accessed is obtained (step 52). To protect a user's identity, the received authentication certificate and prepared access request list are encrypted with a decryption key known only to the user (step 53). Further, an access request packet is generated from the user name, user ID and information encrypted with the decryption key at step 53 (step 54). Thereafter, the access request packet is encrypted with an encryption key of the remote node (step 55). The encryption key is obtained from the encryption key database 2-4 of the authentication server 2. Subsequently, the encrypted packet is sent to the remote file access processing means of the remote node (step 56).

Fig. 6 is a flow chart describing an operation of the remote file access processing means. In Fig. 6, the remote file access processing means 4-3 of the computer system 4 decrypts the received access request packet with a decryption key known only to itself (step 61). Next, it is determined whether the access request packet was successfully decrypted (step 62). If it turns out that it was not successfully decrypted, the procedure goes to step 69, where it is decided that either the request was intended for another node or a third party intercepted the data on the network, and the remote file access processing is denied and aborted (step 69). On the contrary, if it was successfully decrypted, a user name of the source of the access request is retrieved from the access request packet and an encryption key of the user is obtained from the encryption key database 2-4 of the authentication server 2 using the retrieved user name (step 63). Further, the access request list is decrypted with the thus obtained encryption key (step 64). Next, it is determined whether the access request list was successfully decrypted (step 65). If it turns out that it could not be decrypted, it means that it was either an access request from another user or there was intervention by a third party, because the access request list is encrypted with a decryption key of the access requesting user known only to the access requesting user and thus,

the access request is denied and the remote file access processing is aborted (step 69). On the other hand, if the access request list was successfully decrypted, the authentication certificate is retrieved from the access request list and the validity of the authentication certificate is determined from the time of issuance and expiration date of the certificate contained in the authentication certificate (step 66). If the validity of the authentication certificate cannot be verified, the remote file access processing is denied similarly to the step 55 and the processing is aborted (step 69). On the contrary, if the validity of the certificate is verified, it is determined from a user identifier (user ID) and access authorization list owned by the remote file access processing means 4·3 whether file access should be authorized (step 67). When access authorization under the user ID is not registered in the access authorization list, the file access is denied similarly to the step 66 and the access processing is aborted (step 69). On the contrary, if it is registered, the file access is authorized (step 68).

Next, it will be specifically explained how to determine the validity of an authentication certificate at the step 66. Fig. 7 is a flow chart describing an operation of determining the validity of an authentication certificate. In Fig. 7, a user name and user ID are first retrieved from the authentication certificate (step 71) and it is determined whether they agree with the user name and user ID in the file access request packet (step 72). If they do not agree, the certificate is processed as a fraudulent authentication certificate (step 76). On the contrary, if they agree with the user name and user ID in the packet, current time Tc, time of issuance Tt and expiration date T1 are retrieved (step 73). Next, it is determined whether the following expression (1) holds (step 74):

Time of issuance Tt $\leqq$ current time Tc $\leqq$ time of issuance Tt + expiration date T1 (1)

If the expression (1) holds, the certificate is processed as a valid authentication certificate (step 75). If not, the certificate is processed as a fraudulent certificate (step 76).